



---

# Department of the Interior

## IRM Strategic Plan

---

**DRAFT**

May 15, 2013

## Table of Contents

<b>1</b>	<b>Executive Summary .....</b>	<b>1</b>
<b>2</b>	<b>Agency Strategic Goals and Objectives .....</b>	<b>2</b>
2.1	Agency Strategic Goals and Objectives Supported by the IRM Strategic Plan (AXXA).....	2
2.2	Advancing Strategic Goals and Objectives (AXXB) .....	4
<b>3</b>	<b>Improving Services to Customers .....</b>	<b>7</b>
3.1	Measuring Customer Use and Satisfaction through Analytics (BXXA) .....	7
3.2	Improving Usability, Availability, and Accessibility of Services (BXXB) .....	8
3.3	Advancing Agency Performance Goals (BXXC) .....	9
<b>4</b>	<b>Governance and Management Processes .....</b>	<b>10</b>
4.1	Scope of Governance Process (CXXA) .....	10
4.2	Involvement of Agency Stakeholders (CXXB) .....	10
4.3	Valuation Methodology (CXXC) .....	13
4.4	Alignment with DOI Goals and Priorities (CXXD).....	13
4.5	Investment Assessment Process (CXXE).....	14
4.6	Investment Decision Coordination (CXXF) .....	14
4.7	IT Strategic Sourcing Plan (CXXG).....	14
<b>5</b>	<b>CIO Authorities .....</b>	<b>19</b>
5.1	Implementing CIO Authorities through Agency Policies and Procedures (DXXA).....	19
<b>6</b>	<b>Cybersecurity Management .....</b>	<b>22</b>
6.1	Alignment with Cybersecurity Priorities (EXXA).....	22
6.2	Continuity of Operations (EXXB) .....	24
<b>7</b>	<b>Workforce .....</b>	<b>25</b>
7.1	IT Human Capital Planning (FXXA).....	25
<b>8</b>	<b>Managing Information as an Asset .....</b>	<b>26</b>
8.1	Supporting Interoperability and Openness (GXXA).....	26
8.2	Controlling Accessibility to Personal Information (GXXB).....	27
<b>9</b>	<b>Commodity IT and Shared Services.....</b>	<b>30</b>
9.1	Maturing the IT Portfolio (HXXA) .....	30
9.2	Reinvesting Savings from Commodity IT Consolidation (HXXB).....	32
9.3	Maximizing Use of Inter- and Intra-Agency Shared Services (HXXC) .....	33
9.4	Critical Application COOP (HXXD).....	34
9.5	Web Services, Mobile Optimization and Digital Services (HXXE).....	34
<b>10</b>	<b>Privacy.....</b>	<b>39</b>
10.1	DOI's Privacy Approach (IXXA).....	39
<b>11</b>	<b>Accessibility.....</b>	<b>42</b>
11.1	Creating a Diverse Work Environment (JXXA) .....	42
11.2	Integrating Accessibility into IT Processes (JXXB).....	42
11.3	Building Workforce Skills to Support Section 508 Compliance (JXXC) .....	42

---

---

## Table of Figures

Figure 1: Agency Strategic Goals .....	3
Figure 2: Agency Strategic Goals .....	11
Figure 3: Investment Assessment Framework .....	14
Figure 4: Annual Improvement of Strategic Sourcing .....	16
Figure 5: Basic Repeatable Process for Strategic Sourcing.....	17
Figure 6: Decision Making Process for Strategic Sourcing .....	18
Figure 7: UTSP Services.....	32

## Table of Tables

Table 1: DOI Strategic Plan Performance Measures .....	5
Table 2: Initial Strategic Sourcing Areas for Consideration .....	15

## 1 Executive Summary

The Department of the Interior (DOI), the agency responsible for managing America's natural and cultural resources, operates on a \$12 billion annual budget and generates billions of dollars in revenue each year. The Department is also accountable to the public for approximately \$1 billion invested in information technology (IT). Historically, DOI's information resource management programs have operated in a highly federated fashion with much of the management authority distributed throughout bureaus. In December 2010, former Department of the Interior Secretary Salazar issued Secretarial Order 3309 to redirect the oversight, management, ownership, and control of IT infrastructure and the information resource management areas contained in the Clinger-Cohen Act to the Department's Chief Information Officer (CIO).

In January 2011, the Department began its IT Transformation (ITT) Program, a multi-year program intending to significantly improve the cost effectiveness of information technology functions as well as shift from commodity-based technology management to service-based management. The DOI OCIO has been making steady progress toward realizing the vision of Secretarial Order 3309 and is transforming the perspectives of IT leadership at the Department from policy and oversight into Department-wide holistic planning and execution.

This IRM Strategy is organized around the required elements of OMB Memorandum M-13-09, Fiscal Year 2013 Portfolio Stat Guidance: Strengthening Federal IT Portfolio Management and covers a range of Information Resource Management topics beyond those typically considered strategic planning, including:

- Agency Strategic Goals and Objectives
- Improving Services to Customers
- Governance and Management Practices
- CIO Authorities
- Cybersecurity Management
- Workforce
- Information Management
- Commodity and IT Shared Services
- Privacy
- Accessibility
- Enterprise Roadmap

---

## 2 Agency Strategic Goals and Objectives

DOI information technology provides support to virtually all DOI strategic goals and objectives. More specifically, DOI's information technology programs and investments support one of DOI's mission areas: Building a 21st Century Department of the Interior. In turn, it directly supports one of its goals: Increasing the Dependability and Efficiency of Information Technology. Other goals with a strong linkage and dependence on information technology within this mission area include Building a 21st Century Department of the Interior and Sustainability of Interior Operations. IT also plays a major role in another one of DOI's mission areas: Provide a Scientific Foundation for Decision Making. Corresponding goals include Provide Scientific Data to Protect and Inform Communities and Develop a Comprehensive Science Framework for Understanding the Earth.

### 2.1 Agency Strategic Goals and Objectives Supported by the IRM Strategic Plan (AXXA)

---

The DOI CIO is committed to focusing efforts on strategic results and has developed a strategic and performance framework to achieve this effect. The current components of that framework include the following.

#### **Mission:**

DOI's Office of the Chief Information Officer provides excellent, efficient, mission-focused IT services to the employees, bureaus, and offices of the Department of the Interior.

These services include setting overall IT policy; managing the Department's IT portfolio; planning, designing, and delivering IT services; and protecting the Agency's information.

#### **Vision:**

The OCIO modernizes mission support with 21st Century IT by:

- Delivering uniform, modern, agile, and cost-effective services in support of the Department's diverse missions.
- Delivering and managing IT services that empower employees to responsibly steward the natural, cultural, and historic resources with which we have been entrusted.
- Planning, designing, and managing services and investments to drive value and consistency and to align with federal laws, rules, regulations, and directives.

#### **Shared Values:**

- Respecting and valuing employees: The talent, passion, and commitment of our employees are what make it possible for OCIO to provide organizational and service excellence. We strive to be an employer of choice to attract and retain the best workforce. We foster an inclusive and caring environment that encourages engagement, openness, learning, and growth by empowering employees and promoting a work/life balance.
- Mission- focused: OCIO exists to deliver excellent services to customers that enable the success of DOI's missions. Our services and actions must be built with the participation and support of our program customers so that they are responsive to mission needs. We must seek out customer and stakeholder feedback to continuously improve what we do.
- Integrity: We conduct ourselves ethically and responsibly. Our high standards of conduct will be reflected in the quality of everything we do.

- **Accountability:** We take pride in, ownership of, and accountability for our actions to maintain the trust and confidence of those who depend on us as a service provider, corporate citizen of the agency, or steward of taxpayer dollars. We make and keep our commitments to achieve results for the organization.
- **Openness and Transparency:** Honesty and openness to express differing opinions or share new ideas must always be honored so that we are able to consider constructive feedback or critiques and make changes if needed. This is part of building trust and confidence in our people, services, and organization.
- **Economy:** OCIO is a steward of customer resources and commits to managing its resources so that we use what we need and no more. We recognize that our reputation and trustworthiness is earned by demonstrating that we spend wisely to maximize value and return savings to the mission.
- **Excellence:** We strive for excellence in all that we do.
- **Innovation:** We stay tuned into meaningful new innovations from industry, government, or within the agency and introduce these into DOI as best makes sense for us. The world is constantly changing and we must always be open to adopting new ideas that benefit our missions and constituents.

The Agency's Strategic Goals are represented in Figure 1 - Agency Strategic Goals below.

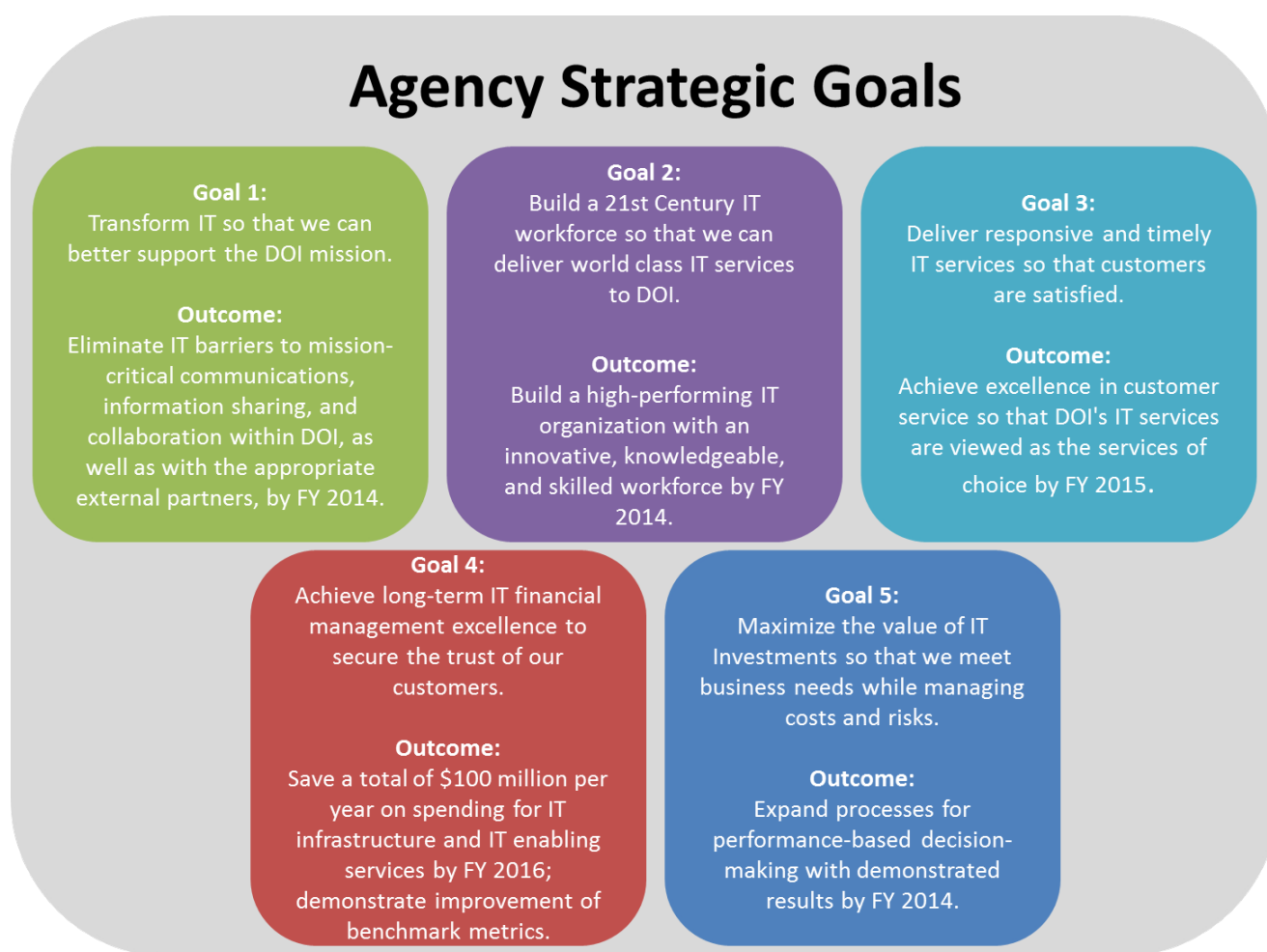


Figure 1: Agency Strategic Goals

---

## 2.2 Advancing Strategic Goals and Objectives (AXXB)

---

Information Technology supports every facet of the Department's diverse missions. Employees, volunteers, and the public require modern, reliable, and agile IT services that can be delivered in a cost-effective and transparent manner. With its redirection of oversight, management, ownership, and control of all Departmental information technology infrastructure in the Office of the Chief Information Officer, Secretarial Order 3309 (Order), issued in December 2010, provided an unprecedented opportunity to change the organization, management approaches and governance of infrastructure at the Department of the Interior. During FY 2013 and beyond, the Department will continue to implement a series of technology innovations and efficiencies as part of an enterprise-wide program of IT Transformation.

The 2013 planned actions do not reflect downward adjustments based in enactment of the Consolidated and Further Continuing Appropriations Act, 2013 (P.L. 113-6) or those required under the March 1, 2013 Sequester Order required by the Balanced Budget and Emergency Deficit Control Act as amended by the Budget Control Act of 2011. Thus, the funding and performance information is overstated as compared to expected actuals.

The following Strategic Actions were planned during FY 2012 and FY 2013.

- Release detailed plan for IT Transformation.
- Establish an IT workforce plan that positions the Department to effectively deliver IT services in a consolidated IT environment.
- Complete the integration of Tier III email support with the OCIO's service delivery organization.
- Complete the migration of bureaus and offices from legacy email services to the unified messaging system.
- Evaluate and select commercial and government hosting options, including cloud and virtualization.
- Continue to evaluate data centers and applications as part of ongoing identification of candidates for consolidation.
- Reduce redundancies and duplicative services at 172 collocated sites, including telecom data circuits
- Engage commercial and government service providers to provide consolidated infrastructure services, such as asset management.
- Implement a service-based cost model that allows managers to choose an appropriate level of service for their needs and budget.
- Publish a service catalog with explicit pricing and features for IT services, including hosting, collaboration, and messaging.

DOI has also planned Actions for the 2014 Fiscal Year, as detailed below.

- Execute the detailed IT Transformation plan.
- Continue establishing an IT workforce plan that positions the Department to effectively deliver IT services in a consolidated IT environment.
- Operate the Tier III email support which has been integrated with the OCIO's service delivery organization.
- Implement selected commercial and government hosting options, including cloud and virtualization.

- Continue to evaluate data centers and applications as part of ongoing identification of candidates for consolidation.
- Continue reduction of redundancies and duplicative services at 18 collocated sites, including telecom data circuits.
- Continue engagement of commercial and government service providers to provide consolidated infrastructure services, such as asset management and other services.
- Operate published service catalog IT services which have been placed into production, using established cost models.

In March 2012, OMB updated the definition of a data center to remove any language that excluded sites less than 500 square feet. Based on this definition update, DOI re-baselined its current Data Center inventory to 406 sites from the original metric of 210 data centers. As a result, the original metric has been updated and DOI is now committed to consolidating 95 data centers.

DOI's Unified Messaging effort experienced a significant re-baselining in FY 2012 following the resolution of Federal Claims Case Number 10-743C, which prohibited the agency from acting on a planned procurement of cloud email services. With resolution of the lawsuit, DOI shifted its focus from implementing a Unified Messaging model predicated on delivering an on-premise, "interim" solution to instead conducting new market research, determining that cloud-based email services best met the agency's need, and issuing a new RFP. DOI awarded a new contract for cloud-based email services in April 2012, rebaselined its Unified Messaging project, and began migrations to the cloud-based system in late FY 2012. As a result, prior year reporting and metrics for the agency's Unified Messaging project do not apply. Despite the significant change in scope these efforts suggest, at the close of FY 2012, DOI had migrated 2,400 of its key IT staff to the new cloud-based solution and the agency remains on target to complete migrations of its entire employee base in early FY2013. To support these efforts, DOI's Strategic Plan Performance Measures are detailed in Table 1 below.

**Table 1: DOI Strategic Plan Performance Measures**

DOI Strategic Plan Performance Measures	Office	2008 Actual	2009 Actual	2010 Actual	2011 Actual	2012 Target	2012 Actual	2013 Target	2014 Target
Percent change in operating costs (as a percentage of total IT spending as reported in Exhibit 300) by consolidating and centralizing the IT infrastructure across the Department, as measured by the reduction in the number of data center facilities, servers, and telecom data circuits from the FY2010 base.	PIO	TBD	TBD	TBD	No Report	No Target	No Actual	No Target	No Target
Percent change in the number of DOI data centers to 115 from FY2010 base of 210.  (New Measure: Percentage of DOI committed 95 data centers consolidated)	PIO	UNKNOWN	UNKNOWN	210	-6.2% 197/210	-13.8% 181/210	No Actual	No Target	No Target
				0%	17.8%	28.4%	44.2%	55.8%	69.5%
				0/95	17/95	27/95	42/95	53/95	66/95

Transition of all DOI employees to a unified messaging and collaboration solution (e.g., email, collaboration, virtual meeting, etc.)	PIO	0	2500	15,000	12%	90%	3.12%	100%	No Target
					10,000/ 82,000		2400/ 76,972	76,972	

While IT activities are frequently beset by risk given the nature of innovation and rapid change, the following specific risks are highlighted for their potential impacts on the realization of established goals and objectives.

- Sequestration and the resulting reduction of resources directly impact our ability to meet our financial goals. While the exact impacts are yet to be determined, they pose a direct challenge and risk.
- Geographically dispersed and independent IT infrastructures in ten bureaus and multiple offices.
- Lack of centralized control over IT spending and development.
- Internal organizational resistance to change.

---

### 3 Improving Services to Customers

DOI has adopted a service delivery model based on industry standard IT Service Management (ITSM) best practices. Customer input is directly integrated into all phases of DOI's service delivery framework from initial strategy to decommissioning, and DOI takes a Balanced Scorecard approach to performance management for all Enterprise IT Services. A major component of the ITSM framework DOI has adopted is Continual Service Improvement (CSI). The CSI processes are designed to collect and consolidate input from customer advisory boards and major stakeholder groups, data from capacity and demand management systems, Enterprise Service Desk reports, and various other feedback mechanisms to help determine needs for new services as well as to improve services already delivered by the Enterprise.

#### 3.1 Measuring Customer Use and Satisfaction through Analytics (BXXA)

---

DOI's OCIO has multiple ongoing sources to obtain customer input into our existing and planned IT services. From in-person meetings to inbox analysis, these sources provide an inclusive overview of customer satisfaction.

Our primary sources of input are regularly scheduled meetings with IT leaders from across the agency who represent IT needs for each of DOI's bureaus and offices. In addition to these weekly meetings, non-IT executives from across the Department participate in monthly IT Transformation Executive Steering Committee meetings and quarterly meetings with Bureau Deputy Directors to make sure we are engaging stakeholders at multiple levels.

In order to maintain an on-going pulse on the day-to-day status of customer satisfaction, direct engagement with customers through dedicated email accounts and regular reports from DOI's various help desk organizations are used to provide quantitative measurements of customer usage and satisfaction levels. The CMO office also facilitates annual Town Hall meetings to provide an opportunity for all employees to hear directly from Senior IT leaders as well as to provide additional input and feedback to the organization.

The Interior Business Center (IBC) performs as a Shared Service Provider and continues to streamline internal processes by using technology to improve our human resources management and financial services as well as extend these improvements to other Agencies through the Human Resources Management LOB and the Financial Management LOB. IBC Human Resources Directorate (HRD) has provided payroll and HR services to Federal agencies for 33 years and provides a full range of technical and operational human resources and payroll services to numerous organizations throughout the Federal government. IBC HRD was selected as an e-Payroll provider in 2002 and later awarded their HR LOB Shared Service Provider designation in 2005 as part of the consolidation of human resources services and technology across the Federal government. IBC HRD currently serves 89 customers, 41 of which use IBC's core systems.

The Office of Personnel Management (OPM) launched the Human Resources (HR) Line of Business (LOB) initiative in 2004 to help the Federal government realize the potential of electronic government and significantly enhance human resources service delivery for civilian employees of the Executive Branch. The HR LOB established the HR LOB Provider Assessment to provide an appropriate degree of oversight and meet customer requirements while imposing a practical level of effort on the part of assessment participants. The assessment is not intended to yield a score; rather, it shows how many practices are effectively employed by HR LOB service providers and how many are not. This approach is meant to shift the focus from a finite final score to a view of

---

HR LOB provider practices, revealing the extent to which they are employing business practices that are important to their customers and whether they are making their customers aware of their business practices. A key aim of the assessment is to offer feedback so HR LOB service providers can take actions to improve both their practices and their feedback loops to customers.

The assessment was led by OPM, which fulfilled a key responsibility of its role as Managing Partner of the HR LOB by providing an appropriate level of oversight to HR LOB service providers. The assessment was performed for IBC, an HR LOB designated service provider, and took place from May 2011 to September 2011. IBC HRD was assessed on its ability to deliver on twenty different business practices that HR LOB customers determined to be important, including a strong commitment to customer service. Customers play a primary role in governance by participating in various workgroups, user groups, and executive committees. IBC takes customer feedback into account when making important business decisions, including plans for system changes and updates, terms specified in Service Level Agreements (SLAs), and decisions about bringing in new customers. As new customers are accepted, IBC practices an implementation approach that balances addressing new customer requirements against meeting and delivering on existing customer requirements.

This assessment applies to services and systems in IBC's Human Resources Directorate. The assessment was based on business practices that are considered important by customers of HR LOB service providers. These customers also developed for each practice a set of assessment questions that are meant to illuminate the extent to which a provider is successfully executing these practices. The practices and questions form the basis of the HR LOB Provider Assessment. Over the course of the assessment period, the assessment team employed a number of formal data collection methods. An online questionnaire was used to obtain data from customers. Follow-up interviews were conducted with some customers to obtain additional qualitative information. Information from IBC was obtained via formal interviews. To address customer concerns, IBC implemented the HRD Customer Satisfaction Improvement Plan, which identifies action plans, milestones, deliverables, and responsible parties that report on action items to management. IBC proactively reaches out to customers through multiple methods including their User Group meetings, one-on-one meetings, and phone calls or visits from the client liaisons.

"Considering the assessment results across all assessment categories, NBC is doing an outstanding job, and customer feedback was consistent across all assessment categories. NBC has developed a clear and defined strategic vision – "to be the HR Shared Service Center (SSC) provider of choice in the federal marketplace" – that drives all NBC processes and roadmap activities. This vision is the key to NBC's drive toward continuous improvement. NBC has developed strong customer relationships, and through their broad governance process enables customer involvement in key decisions."

- OPM Human Resources Line of Business Provider Assessment Report, September 2011

### **3.2 Improving Usability, Availability, and Accessibility of Services (BXXB)**

---

Facilitation and management of the organizational customer service improvement and performance management processes are primary responsibilities of the Office of Chief Management Officer. This includes a Customer Management division, a customer-facing organization that manages the various customer advisory boards and coordinates collection and consolidation of all customer feedback data. The Customer Management division is also responsible for actively engaging customers to solicit feedback and quickly address high-impact issues in order to maintain the highest levels of customer satisfaction possible.

---

### 3.3 Advancing Agency Performance Goals (BXXC)

---

The Office of the Chief Management Officer also includes a Performance Management division which is responsible for oversight and guidance for performance management activities across the organization. This includes ensuring that the organization is adhering to the DOI Service Delivery Framework and integrating the appropriate performance measures into all phases of the service delivery lifecycle as well as to ensure that all facets of the Balanced Scorecard methodology are incorporated when developing performance metrics for Enterprise IT Services. The Performance Management division is also responsible for management and tracking of all scorecard activities along with reporting of performance metric data across the organization.

Tools, including the American Customer Satisfaction Index (ACSI), are used by IBC to benchmark against industry standards, and findings have aided IBC in the development of their performance improvement goals. IBC is also ISO: 9000 certified and looks to ISO: 9000 procedures for best practices to include in the IBC security procedures. IBC is the only HR LOB shared service center that provides a fully integrated human resources and payroll solution to their customers. IBC uses industry-based best practices and open standards-based best practices as a basis for up-to-date integration and interoperability standards and guidelines. Employing these practices enables IBC to have a portable, agile, and technology-agnostic technology platform that supports their fully integrated HR system. Furthermore, IBC uses their Human Resource Management Suite HR System Integration Framework (HRMS HR SIF) to connect HR systems hosted by IBC, partner vendors, and customer agencies through a set of HR related business process workflows, business rules, event rules, and routing rules. The underlying technology of HRMS HR SIF is a portal, enterprise service bus, and workflow server.

---

## 4 Governance and Management Processes

Today's fiscal realities force DOI to consider new ways of supporting business and IT Transformation. The IT Transformation is not just concerned with cost, schedule, and performance requirements. It is also focused on increasing DOI's capacity to adapt IT infrastructure services to changing circumstances while still executing and enhancing its mission-critical activities. To make sound and timely transformational decisions, senior DOI leadership requires deep insight into DOI's mission, support service and infrastructure capabilities, and their respective performance levels and costs.

### 4.1 Scope of Governance Process (CXXA)

---

Central to effective IT governance is the establishment of a clearly defined IT decision-making framework. During FY 2010, Secretarial Order 3309 radically changed the scope of IT authorities from a decentralized delegation within the bureaus/offices to a centralized model under the DOI CIO. Component CIOs no longer exist within DOI. This consolidation of authority over IT positioned the CIO with responsibilities and authorities to improve the operating efficiencies of organizational sub-components and DOI as a whole.

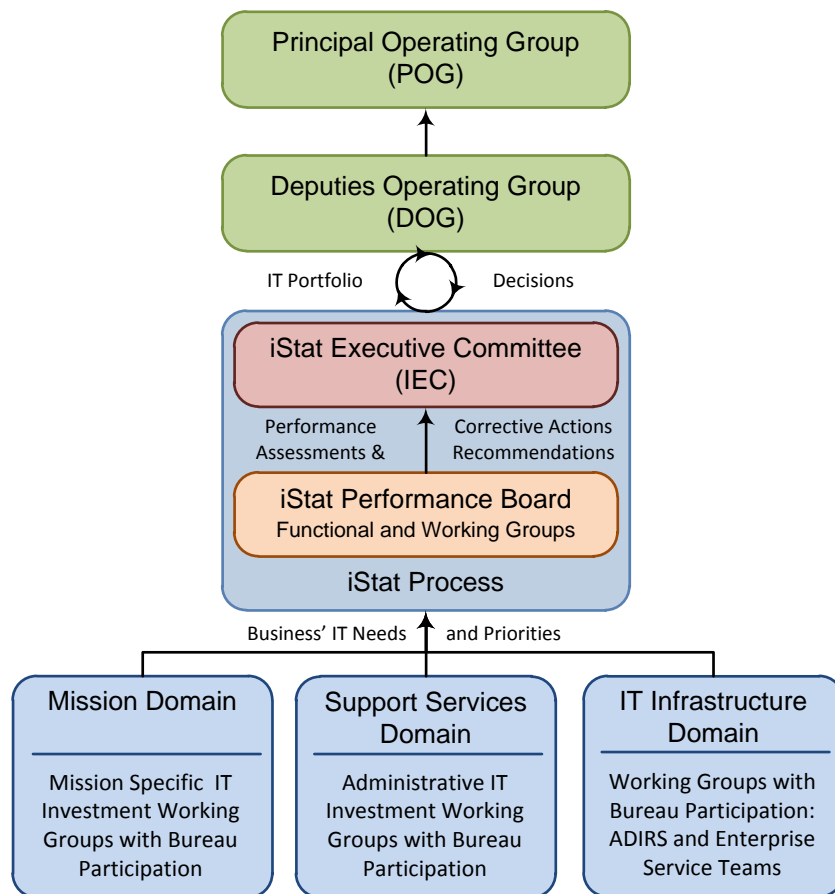
To improve IT governance practices and to close gaps or weaknesses that have been identified through this process or others, a target governance model for managing DOI's IT investment portfolio is being established to enable improved organizational performance, eliminate unnecessary duplication, and realize cost savings. The outcome of the target IT governance model includes collaborative management, with IT investment decisions being made by the business owners with approval by the iStat Executive Committee (IEC) and the Deputies Operating Group (DOG) as appropriate. It also involves IT decisions being directly linked to the management and business needs of the organization. This new model will enable key stakeholders, such as the DOI Chief Information Officer (CIO), in collaboration with the Chief Acquisition Officer (CAO), the Chief Financial Officer (CFO), and Chief Human Capital Officer (CHCO), to be engaged in the governance process and increase bureau/office representation within line of business segment roadmap efforts around each of the domain boards.

DOI's IT governance is focused on measuring IT value, ensuring mission and business effectiveness, enabling data-driven decisions around commodity IT investments, and setting clear targets for IT spend reductions and consolidations. DOI's IT governance reform also supports overcoming bureaucratic impediments to deliver enterprise-wide solutions that can drive down costs and achieve great efficiencies.

### 4.2 Involvement of Agency Stakeholders (CXXB)

---

Figure X below demonstrates the target high-level IT governance model to which DOI began to transition in 2011. DOI senior leadership is involved in the IT governance and decision-making processes. The Principals Operating Group (POG) is chaired by the Deputy Secretary and is comprised of DOI's Assistant Secretaries, Bureau Directors, and members of the Secretary's staff. The POG replaced DOI's former Management Excellence Council (MEC). The Deputies Operating Group (DOG) is chaired by the Assistant Secretary of Policy, Management and Budget (PMB), who serves officially as DOI's CFO and CAO. The DOG membership is comprised of the Deputy Bureau Directors and PMB's Deputy Assistant Secretaries, including the CAO. The group focuses on operational issues affecting DOI and its bureaus/offices. The DOG replaced DOI's former Management Initiatives Team (MIT).



**Figure 2: Agency Strategic Goals**

The iStat process integrates the IEC and the iStat Performance Review Board, two key bodies of DOI’s IT governance process. As the IEC chair, the DOI CIO drives the investment review process for IT investments and has responsibility over the entire DOI IT portfolio. The iStat Executive Committee (IEC) is the Department-level IT investment review board. The IEC takes into consideration the recommendations from each of the Domains and the iStat Performance Board and makes decisions to eliminate in part or whole wasteful or low-value investments. The IEC looks across Domains (Mission, Support Services, and Infrastructure) to identify any duplication.

The IEC replaced the DOI’s former Investment Review Board (DOI IRB). The DOI CIO chairs the IEC providing direct oversight of the IT portfolio for the Secretary. Per Secretarial Order 3309, the DOI CIO “reports to the Secretary and receives administrative and management guidance from the Assistant Secretary – Policy, Management and Budget, as well as the Deputy Assistant Secretary – Technology, Information, and Business Services. The CIO also receives management guidance from the Deputy Secretary in his or her role as the Department’s Chief Operating Officer.” IEC membership also includes the DOI’s Deputy Assistant Secretaries for: 1) Technology, Information and Business Services, 2) Budget, Finance, Performance and Acquisition, 3) Human Capital and Diversity, and a single rotating member from the Mission domain. This membership

---

composition ensures the IT portfolio is being analyzed as an integral part of the budget process at DOI. The IEC is responsible for directing, controlling, and measuring all DOI Information Resource Management (IRM) resources and risks and optimizing the value of the DOI IT portfolio. The IEC ensures IT investments meet and are driven by the business needs of DOI, the bureaus, and the priorities of the Secretary of the Interior in the most effective and efficient manner.

The iStat Performance Review Board brings rigor and thoroughness to DOI's IT investment management and review functions and is modeled after the Office of Management and Budget (OMB) TechStat review process. The iStat Performance Board performs an in depth review of selected IT investments across LOBs, based on a number of factors, to assess if the investment is realizing its planned value. The iStat Performance Review Board is chaired by the DOI Deputy CIO and membership is comprised of the A-130 functional managers. The purpose of the iStat Performance Review Board is to:

- Improve the performance and accountability of IT investments by providing a comprehensive Departmental review of potentially troubled IT investments as reflected on the Federal IT Dashboard or through internal agency knowledge.
- Determine compliance to Federal regulations and standards.
- Recommend appropriate corrective actions that mitigate risks.

The iStat Performance Board also conducts reviews of similar systems and investments to get a better understanding of what if any duplication exists in order to streamline or reduce redundancies. Finally, the iStat Performance Review Board prepares assessments and recommendations that are elevated to the IEC.

In the target IT governance model, DOI business-driven IT needs and priorities are communicated into the iStat process through three primary domains: 1) Mission, 2) Support Services, and 3) Infrastructure. The goal in all domains is to drive enterprise IT decision-making within specific, cross-cutting business segments (or lines of business) rather than within DOI's formal organizational structures, which tend to be stove-piped. This will help DOI to reduce unnecessary duplication in IT investments, establish enterprise-wide solutions, and improve overall performance. Membership in the governance process focuses on gathering people with decision-making authority and allowing greater bureau participation through contribution as subject matter experts through roadmap development efforts. DOI has developed several line of business segment roadmaps that enable governance decisions and ensure investment decisions are aligned with the approved roadmap direction. This model aligns with and supports the three OMB identified IT Shared Service categories, which correspond directly with the three domain boards. Their activities will add value and support the evolution to the target model.

- **Mission IT:** Following recommendation from an iStat Performance Board, a Trust Executive Committee was established and is chaired by the DOI CIO, Directors for the Office of Special Trustee (OST), and the Bureau of Indian Affairs (BIA) to oversee and enable IT decisions that further Indian Trust mission requirements. Additionally, with the addition of DOI's Geospatial Information Officer, an effort is underway to drive consolidation and achieve greater efficiencies through geospatial solutions across DOI and as a Shared Service.
- **Support IT:** The Office of the Secretary Investment Review Board (OS IRB) is transitioning to the Support Services Board. Currently, this board is leading the development and implementation of six line of business segment roadmaps.

- 
- **Commodity IT/IT Infrastructure:** An IT Transformation Executive Steering Committee (ESC) has been established to provide direction and oversight of IT Transformation and the consolidation around IT infrastructure.

Activities and recommendations at the mission, support services, and IT infrastructure levels roll up to the other governance layers that are looking across the IT portfolio to make comparative decisions that will enable DOI to successfully move towards application rationalization and service orientation.

DOI is currently in the process of transitioning towards the target state governance model through a set of discrete actions. The IEC, the iStat performance board, and the Support Services Board (SSB) are operational. The IT Transformation ESC is focused on IT infrastructure commodity consolidation activities, which will evolve into the IT infrastructure domain.

### 4.3 Valuation Methodology (CXXC)

---

In general, the criteria used for investment and system valuation to identify wasteful or low-value investments and for targeting duplicative systems is defined by the stakeholders performing the analysis. Depending on the perspective of the analysis being performed, whether it is Bureau, LOB (cross-bureau and office), OCIO, DOI, or Federal-wide, the relevant goals and objectives are taken into account as a value measure. Cost, schedule, and time to realize value are all widely utilized.

Bureaus and offices each have their own investment review boards (IRBs) and leverage investment and system valuation models when making recommendations to leadership within their respective bureaus and offices on wasteful or low-value investments. At the Department level, DOI has historically leveraged investment and system valuation models across Bureau and Office portfolios. However, due to a number of factors inclusive of governance challenges and subsequent transition to the target state model, the use of these models is being folded into lower level governance processes. Specifically, LOBs are beginning to use valuation models during the development and maintenance of segment roadmaps. An example of this is the Workplace Computing Services (WCS) prioritization. In support of the WCS team, the DOI Enterprise Architecture (EA) Program helped to establish an IT Transformation performance-driven prioritization framework to measure the IT Transformation efforts. The EA team took a “ruthless prioritization” approach that aligned priorities with the IT Transformation goals. The priorities were evaluated by clear IT Transformation goals and expected outcomes and supported by successive versions of architectures, plans, and solutions.

### 4.4 Alignment with DOI Goals and Priorities (CXXD)

---

On an annual basis, during the development of the IT budget, DOI leverages a budget request form to collect information from the bureau and office investment/system owners with regard to the alignment of their investment/system with the DOI mission and business functions. In addition, the EA Program is responsible for mapping all investments to the OMB Business Reference Model and the DOI Business Model. This ensures that mapping of DOI’s investments to the DOI mission and business functions are performed consistently across the entire portfolio. Bureaus and offices are provided the ability to request adjustments or changes to the mapping of their investments. In addition, during the development and maintenance of LOB segment roadmaps, segment leadership and the roadmap support team ensure that the investments and systems are accurately aligned with the LOB business functions.

---

#### 4.5 Investment Assessment Process (CXXE)

---

The framework that is generally leveraged for all investment and system valuations and was specifically used for WCS is represented in Figure 2 below.



Figure 3: Investment Assessment Framework

#### 4.6 Investment Decision Coordination (CXXF)

---

DOI's Enterprise Architecture program is engaged in identifying wasteful and low-value investments and identifying duplication through various perspectives and governance levels at DOI. The EA program leverages various taxonomies, including OMB reference models and DOI's internal Business Model, to characterize investments and systems to identify commonality and duplication. The EA program is a service provider to the DOI LOBs to provide development and maintenance of the segment roadmaps. The EA program facilitates investment and system valuations within each LOB and brings the enterprise-wide perspective to the analysis as well. In addition, the EA program is a member of and participates in iStat Performance Board reviews specifically with the purpose of offering recommendations regarding the value of the investments/systems and alternatives that may exist.

#### 4.7 IT Strategic Sourcing Plan (CXXG)

---

As the IT community identifies what would be potential opportunities for strategic sourcing, the OCIO must engage the acquisition community to develop an acquisition strategy.

As part of the development of an acquisition strategy, the OCIO and acquisition community need to secure and analyze data on existing contract vehicles (GWACs, DOI-wide, Bureau-wide) that could be utilized - OR – need to identify the parameters of existing contracts in determining path forward (i.e., contract length, commodity/service). This will help to identify use of existing vehicles or the need for development of new vehicles for DOI.

##### Initial Strategic Sourcing Targets

Initial analysis and discussion with Bureau IT leaders targets the following areas of focus for IT Transformation Strategic Sourcing initiatives. More in-depth analysis of the business and technical requirements is necessary in order to finalize target sourcing opportunities.

Table 2: Initial Strategic Sourcing Areas for Consideration

Telecommunications	Hosting Services and Workplace Computing	Account Management	Enterprise Service Desk
<b>Cellular Services</b>  <b>Voice</b> Voice Conferencing PBX VOIP Handsets PRI Circuits (PRI = Primary Rate Interface) Maintenance  <b>Video</b> Software Hardware including Bridges and Switches Cameras TelePresence PRIs Maintenance  <b>Local Area Network</b> Hubs, Switches, Routers Wireless Access Points (AP) Maintenance Software  <b>Wide Area Network</b> Circuits Routers, Switches Maintenance  <b>Radio</b> Radio (Devices, Hardware)	<b>Enterprise Hardware</b> Laptop, Desktop, Monitors, Storage Area Network Servers  <b>Enterprise Software</b>  <b>Hosting Services</b> Application Hosting  <b>Professional Services</b> Enterprise Architecture/ Strategic Planning Capital Planning	<b>Identity Management and Access Control</b>	<b>Enterprise Service Desk CRM/Software</b>  <b>Enterprise Service Desk Services</b>

The following outlines the general approach for evaluating and pursuing strategic sourcing initiatives:

- ☑ Collect data from each Bureau/Office categorically by each IT Transformation Area, product service type, and alignment to the IT Portfolio. This is the early phase of the roadmap and approvals of the acquisitions are mostly favorable because executable IT Transformation solutions are pending.
- ☑ Extract data that lists common solutions acquired throughout DOI, highlight solutions that can be leveraged or eliminated as enterprise solutions become available.
- ☐ Develop managed service model
- ☐ Determine funding model to be used for maximum savings
- ☐ Streamline and align reporting methods to achieve consistency and avoid redundancy
- ☐ Centrally post enterprise solutions on the portal
- ☐ Issue policy on the mandatory use of enterprise solutions
- ☐ Phase-out of the process to review IT acquisitions that can be acquired from enterprise solutions
- ☐ Monitor the success of the managed service model

The outcomes stated below enable the fulfillment of the organizational change model illustrated in the IT Transformation Strategic plan.

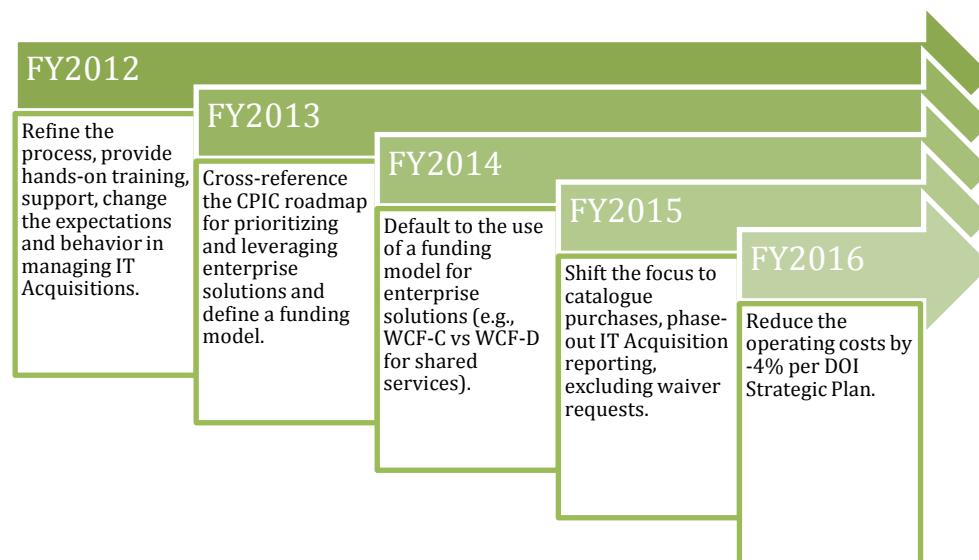


Figure 4: Annual Improvement of Strategic Sourcing

## Strategic Sourcing Process and Evaluation

Consistency of approach is important to realizing the overall strategic sourcing vision. DOI has established a basic repeatable process for strategic sourcing. Below is an illustration of the major milestones that can be reused when planning for most enterprise solutions.

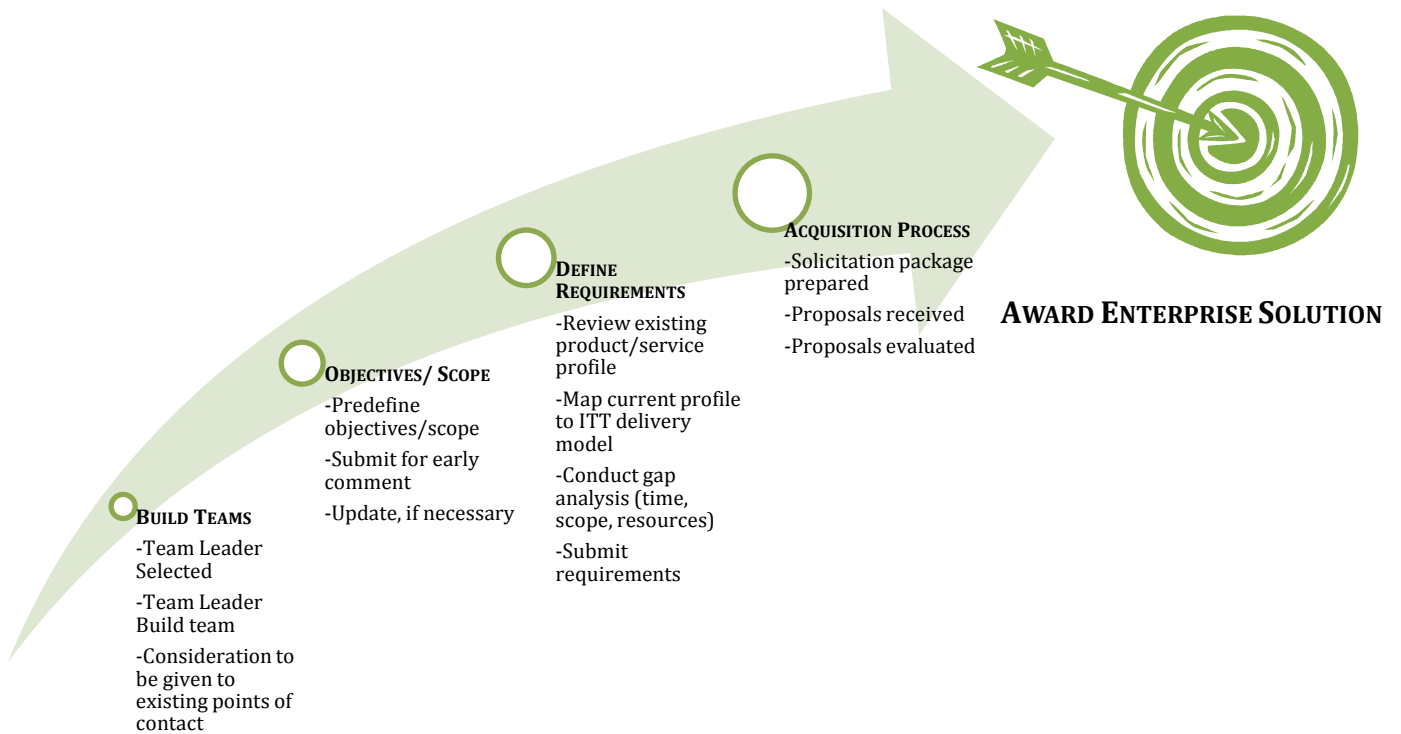


Figure 5: Basic Repeatable Process for Strategic Sourcing

In addition to the basic repeatable process DOI has adopted a decision making process for evaluating potential opportunities for strategic sourcing.

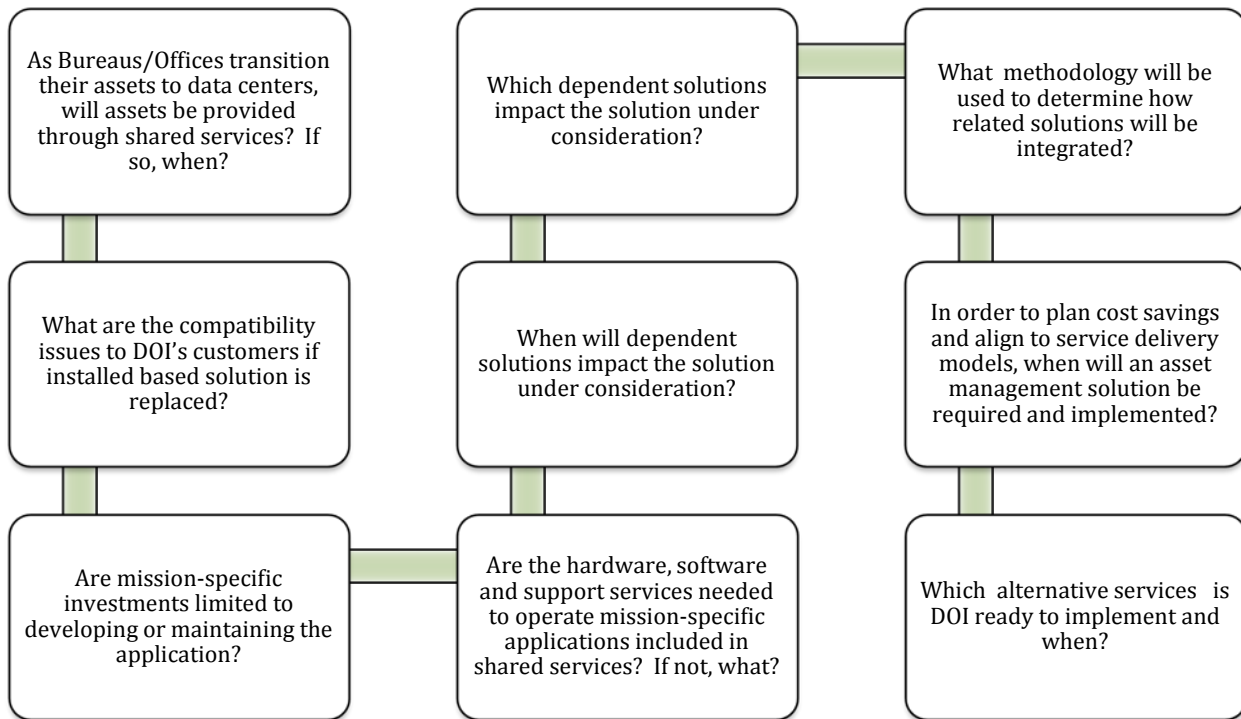


Figure 6: Decision Making Process for Strategic Sourcing

---

## 5 CIO Authorities

### 5.1 Implementing CIO Authorities through Agency Policies and Procedures (DXXA)

---

The DOI CIO has the critical authorities currently available through law and policy. However, complex management models and extra layers of bureaucracy impede his ability to execute effectively and efficiently. Impediments to Agency CIOs' ability to execute on the demands of 21st century management challenges can be overcome through direct line authority of IT budgets and control of IT staff. Significant opportunities for improvements in cost efficiency and interoperability of information management will remain unrealized without clear lines of accountability and authority. Today, unnecessary layers of bureaucracy cause barriers to aligning resources and inhibit authoritative decision-making. This bureaucracy creates overly complex channels of communication and too many players and steps in the decision-making process, which further confounds the agency's ability to effectively execute modernization efforts. In Veterans Affairs, which is the only agency to date with this authority, the authority over IT budgets and staff has delivered significant improvements in oversight and management, which has resulted in improvements to mission effectiveness.

Consistent with FY14 passback direction, the DOI OCIO has completed the following activities.

#### Gap Analysis

The Office of the Chief Information Officer (OCIO) conducted a gap analysis to determine if the Department of the Interior (DOI) Chief Information Officer (CIO) was properly positioned with appropriate responsibility and authority to improve IT operating efficiency throughout the Department. The gap analysis conducted by OCIO was based on authorities identified in Government Accountability Office (GAO) Report GAO-11-634, Federal Chief Information Officers, Opportunities Exist to Improve Role in Information Technology Management, as well as Office of Management and Budget (OMB) Memorandum M-11-29, Chief Information Officer Authorities.

On December 14, 2010, Secretary Salazar issued Order Number 3309, Information Technology Management Functions and Establishment of Funding Authorities (Order). The Order, Section 7, Delegation of Authority, states, "The CIO has the delegated authority of the Secretary necessary to implement and verify compliance with requirements of the Clinger-Cohen Act, other applicable Federal information technology laws and policies, and this Order."

#### Plan of Action and Milestones

The Order directed the implementation to be completed within four years. In June 2011, the CIO provided to Secretary Salazar an Information Technology (IT) Strategic Plan that summarized the steps necessary to fully implement the Order by December 14, 2014. An IT Transformation Initiative has been underway for more than two years and is expected to realign the resources under the CIO necessary to fully implement the authorities contained in law and policy. Planned key milestones are provided below; however it should be noted that they may change over time due to sequestration or other emerging constraints.

#### FY2013

- Chief Management Office (CMO): (Q3) Implement Shared Service Portfolio & Strategic Communications Management; (Q4) Implement Customer Relationship, Performance & Change Management, Governance
- IT Shared Services Organization (ITSSO): Telecom - (Q2) Simplify and Upgrade WAN

- ITSSO: Hosting - (Q4) Commercial Cloud Contract
- OBS: (Q3) Department-wide IT Strategic Sourcing initiative chartered; target sourcing opportunities identified; (Q4) Strategic Sourcing planning finalized

#### FY2014

- ITSSO: End User - (Q1) Implement Enterprise SCCM; (Q2) eERDMS Support; (Q4) Implement Enterprise Directory Services
- ITSSO: Enterprise Service Desk - (Q1) Enterprise Services for Unified Messaging; (Q4) Implement Additional Services
- ITSSO: Hosting - (Q1) Hosting Study Findings Implemented and Operating at Enterprise
- ITSSO: Information Assurance - (Q1) Implement Enterprise Secure File Transfer Solution; (Q3) Implement Enterprise Encrypted Traffic Intercept
- ITSSO: Telecom - (Q4) Enterprise Cellular Services
- Geospatial (GEO): (Q1) Provide OS Geospatial Support; (Q2) Implement Policy, Strategy and Enterprise Licensing; (Q4) Implement DOI Shared Geospatial Infrastructure
- OCIO Business Services (OBS): (Q1) Finalize Workforce Planning Initiative; (Q4) Implement IT Enterprise Software Sourcing
- Policy, Planning and Compliance (PPC): (Q3) Implement Enterprise Records Management Program; (Q4) Implement Enterprise Information Assurance Program to include Policy /A&A

#### FY2015

- ITSSO: Information Assurance - (Q1) Implement ICAM Logical Access, Physical Access & Federated Access; (Q4) Implement Enterprise SIEM Solution, Continuous Monitoring
- ITSSO: Telecom - (Q2) Strategic Sourcing; (Q4) Implement Enterprise LAN, Voice/Video Services,
- ITSSO: End User - (Q3) Implement Local Desktop Support Strategy
- OBS: (Q1) Implement IT Enterprise Hardware Sourcing
- PPC: (Q1) Implement Enterprise Capital Planning & Investment Control, Policy Management; (Q4) Contract Consolidation and Contract On-Demand/Fee for Service Support

#### FY2016

- ITSSO: Information Assurance - Implement Enterprise Continuous Monitoring

### **Summary of Proposal**

This proposal describes how DOI can realign and improve funding requests, budget execution, and financial reporting for IT expenditures to better track planned and expended resources for IT goods and services. It also ensures that CIOs have both direct control over all commodity IT spending and appropriate oversight of all IT-related funding requests and budget execution.

The Order, Section 6(g) states, "All IT procurement expenditures, over the micro-purchase level, must have the approval of the Office of the Chief Information Officer before funds are obligated via any approved method." In adhering to the Order, DOI developed guidance and internal controls which require IT requirements be

---

submitted for a review before products or services can be acquired by any organizational element within DOI. The following objectives have been defined to mature the review and approval of funding requests and increase efficiency and cost savings in IT-related expenditures.

- Collect data from each Bureau/Office categorically by each IT Transformation Area, product service type, and alignment to the IT Portfolio.
- Extract data that lists common solutions acquired throughout DOI and highlight solutions that can be leveraged or eliminated as enterprise solutions become available.
- Develop managed service model (planned completion date to be determined).
- Determine funding model by September 2016.
- Streamline and align reporting methods to achieve consistency and avoid redundancy by September 2014.
- Centrally post enterprise solutions on the portal (ongoing).
- Issue policy on the mandatory use of enterprise solutions by September 2013.
- Phase-out of the process to review IT acquisitions that can be acquired from enterprise solutions by September 2013.
- Monitor the success of the managed service model (planned completion date to be determined).

#### **Document Formal Agency Policies**

Departmental Manual (DM), Part 112, Chapter 24, Office of the Chief Information Officer, January 14, 2011, Section 24.4 states, “The purpose of the Office of the Chief Information Officer (OCIO) is to establish and manage a comprehensive information resource management (IRM) program for the Department of the Interior. The basic elements of the program include policy, planning, execution, oversight and service delivery. This includes defining standards, guidelines, metrics, and processes for ensuring compliance.”

---

## 6 Cybersecurity Management

The DOI CIO has the authority and primary responsibility to implement an agency-wide information security program and to provide information security for both the information collected and maintained by the agency and for the information systems that support the operations, assets, and mission of the agency. This includes well-designed, well-managed, continuous monitoring and standardized risk assessment processes that are augmented by "CyberStat" sessions.

### 6.1 Alignment with Cybersecurity Priorities (EXXA)

---

The following describes how DOI addresses the extent to which IT security activities may be consolidated under the DOI CIO. As a result, the CIO is able to address IT security activities. Secretarial Order 3309 states:

*"The CIO will assume oversight, management, ownership, and control of all Departmental IT infrastructure assets including, without limitation, externally hosted or managed IT services and the delivery of managed services for the use and benefit of the Department, its bureaus, offices, and other authorized beneficiaries or the equivalent thereof."*

*"Infrastructure" refers to the collection of systems, components, and services that are necessary for electronic data storage, processing, and transmittal of data. Any equipment connected to any DOI network is an asset of the DOI Infrastructure. Infrastructure includes, but is not limited to, the network, servers, data centers, workstations (desktops, laptops), printers, telecommunications equipment and all software, hardware, and services necessary to operate those systems."*

In addition, Secretarial Order 3309 includes the following delegation of authority that encompasses the planning and management of IT security throughout DOI:

***"Delegation of Authority.** The CIO has the delegated authority of the Secretary necessary to implement and verify compliance with requirements of the Clinger-Cohen Act, other applicable Federal information technology laws and policies, and this Order; approve all recruitment and reassignment actions for all Information Technology positions within the Department; and establish appropriate governance entities that will have the authority to terminate any IT project as they deem necessary or in the best interest of the Department."*

Secretarial Order 3309 is fundamentally aligned with the Clinger Cohen Act (CCA), which calls for the transfer of all Clinger Cohen functions, including cybersecurity, to the agency's Office of the Chief Information Officer and for these functions to be managed centrally.

IT cross-cuts the entirety of DOI's programs and initiatives; therefore, a stable, agile, and secure IT environment is critical for achieving DOI's mission. To fortify the new alignment of IT security within DOI, an information assurance service area was established to plan and manage IT security at the enterprise level and to deliver it using a service delivery approach. The information assurance service area is pursuing plans and methods for implementing cybersecurity best practices for the enterprise, including the establishment of new IT security policies, the re-architecture of IT security authorization boundaries, the implementation of a robust enterprise continuous monitoring program, and the optimization of DOI's networks to better meet customer needs while improving overall IT security. Duplicative IT security activities that are in place today have previously impeded DOI's desire to deploy enterprise-level security controls that provide opportunities for significant cost savings. Secretarial Order 3309 has also enabled DOI to better facilitate collaboration across several IT

---

functional areas that have led to plans that will result in efficiencies and improvements in overall IT security. These changes are transformative and are not a viable course of action without a central IT authority.

The transfer of authority for IT operations and security processes, systems, and personnel that were previously under bureau control to the CIO is being undertaken carefully to ensure that the appropriate policies and procedures are in place to enable a well-managed, effective implementation over time. In concert with this, DOI is implementing new components of commodity IT investments at the enterprise level while planning and coordinating the decommissioning of duplicative legacy systems in subordinate organizations. These activities require close coordination in the current multi-authority environment. IT workforce management and labor relations considerations, complex planning activities, and subordinate organization resistance have presented challenges to the expeditious implementation of IT consolidations and management centralizations. DOI is keenly focused on strengthening IT governance as a key component to overcoming obstacles while managing risk as it undertakes this ambitious initiative.

DOI's existing IT security goals have historically been based on the Federal Information Security Management Act (FISMA) compliance mandates and have been updated accordingly based on new National Institute of Standards and Technology (NIST) guidance and standards, OMB memorandums, and GAO findings. DOI's plan aligns with DOI's existing IT security goals and, with the implementation of Secretarial Order 3309, has already begun showing positive results for DOI. DOI is over 90% compliant with Trusted Internet Connection (TIC) requirements to date and is utilizing the new information assurance service program to plan and implement an enterprise continuous monitoring program to include near real-time dashboarding of vulnerability and patch management activities across DOI for better visibility and faster response. DOI has also created a new independent verification and validation team responsible for reviewing existing Plan of Action and Milestone (POA&M) activities and working with bureau/office personnel to facilitate better management and more responsive closure of security findings Department-wide.

With the authority for IT under the DOI CIO, the consolidation of the commodity IT infrastructure is underway, which will enable DOI to realize reductions in duplicative IT assets and the removal of bureau-specific IT policies and security frameworks. To address vulnerabilities, DOI updated and implemented its Departmental Manual on the Information Security Program (375 DM 19), which identifies 18 agency-wide standards for IT security and identifies the CIO's designated Authorizing Officials (AOs). These new standards are based on the Revision 3 of the NIST 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, as well as the Federal Risk and Authorization Management Program (FedRAMP) recommended security controls for information systems within Cloud computing environments. This updated handbook and revised Departmental policies are also aligned with NIST Special Publication (SP) 800-37, *Guide for Applying the information assurance Framework to Federal Information Systems*. SP 800-37 calls for the implementation of an information assurance Framework (RMF). The continuous monitoring of security controls is one of the fundamental steps in the RMF process.

DOI is requiring Bureaus and Offices to prepare individual implementation plans for Strong Authentication and Continuous Monitoring. The DOI OCIO will evaluate the plans and facilitate achieving the respective CAP targets and monitor progress toward the targets. With respect to Continuous Monitoring, DOI is engaged in the DHS Continuous Monitoring and Mitigation Program (CDM) and anticipates being one of the early engagement participants; DOI OCIO is directly responsible for achieving the Trusted Internet Connection target. DOI is working with DHS to transition from Einstein 2 to Einstein 3 and the DHS Intrusion Protection Security Service

---

(IPSS). Progress toward the CAP targets is regularly monitored at the DOI leadership level by the Chief Information Officer, the Deputy Assistant Secretary for Technology, Information, and Business Services, the DOI Performance Improvement Officer, and the ICAM Executive Steering Committee.

## **6.2 Continuity of Operations (EXXB)**

---

Currently Interior and its subcomponent organizations provide the proper continuity of operations (CooP) and disaster recovery (DR) capabilities based on the specific requirements of a particular application. Interior is actively pursuing additional means in which CooP and DR requirements can be met more efficiently by utilizing shared resources across all Interior bureaus/offices as well as leveraging other technologies (cloud-based offerings). From a shared services perspective, one of the requirements moving forward with any strategy is the consideration for CooP and DR to meet the mission needs of all of Interior as well as subcomponent organizations.

Interior's cloud-based email and collaboration service takes advantage of the CooP and DR capabilities provided by our Cloud services vendor. The Statement of Objectives for our cloud email services requirement specifically includes language to ensure requirements are included to prevent the loss of DOI data, service degradation, and/or service disruption to DOI users in the event of planned or unplanned outage. To address this, the cloud based vendor is providing:

- Multiple copies of user data made available in real-time to the various Google services through live (or synchronous) replication.
- Simultaneous replication of every action taken in Gmail across multiple servers in at least two data centers.
- Instantaneous transfer of data if a server fails or an entire data center suffers an interruption.
- Zero/instant failover RPO design target.

---

## 7 Workforce

### 7.1 IT Human Capital Planning (FXXA)

---

Interior surveyed its IT workforce in spring 2012 to assess IT capabilities with regards to 1,000+ skills and for proficiencies in 14 behavioral and business competencies. Competencies were selected based on the types of IT and technology management roles performed by IT professionals. By the end of FY13, it is expected that Interior will define additional operational details for the IT future state and identify the related competencies needed to achieve that future state. Interior will compare the IT workforce future state requirements against the IT workforce skills and competency assessment data to determine gaps.

To close the gaps, Interior will develop a comprehensive IT Workforce Training and Development Plan to ensure execution of the IT future state. Interior's Privacy Training Program includes mandatory Privacy Act training as part of the Federal Information System Security Awareness (FISSA) training for all new employees and contractors. Specialized computer-based training courses and individual or group training is also provided. Interior developed The Privacy for IT Personnel course, a computer-based privacy training course for IT personnel in accordance with OMB M-07-16, which requires that agencies provide targeted, role-based training to managers, Privacy Act officers, and employees with privacy responsibilities. DOI continues to focus on the importance of having qualified IT project and program managers. In collaboration with DOI University, DOI offers two certificate programs in support of this focus: 1) Project Management Associates Certificate or Masters Certificate from George Washington University and 2) a FAC-P/PM certification program. Individual classes or the full curriculum resulting in certifications can be pursued.

As stated in M-11-29, *"Agency CIOs shall improve the overall management of large Federal IT projects by identifying, recruiting, and hiring top IT program management talent."* The first milestone in the alignment of the IT workforce is to analyze the capabilities of the existing workforce against the skills required to perform in the transformed IT environment. A key outcome of this analysis will be the identification of critical gaps/excesses in skills, geographic coverage, and numbers of FTEs throughout DOI.

In April 2012, as part of a plan to grow the Program Management job title using an agency-wide process to document challenges and capture best practices and lessons learned, DOI began an inventory of the skills of its IT workforce. The purpose of the assessment was to identify and address competency gaps in order to better understand the skills and competencies within the workforce, specifically as they relate to the support of emerging technology being used in IT Transformation initiatives. One of the skill categories assessed is IT program management. The skills inventory will identify where those program management skills reside as well as highlight developmental areas where additional training will be helpful.

Once the analysis of the workforce is complete, a comprehensive plan will be developed to address the skill gaps, outline training programs, and provide a path for career development within the transformed IT organization. As services are established and consolidated through implementing the service delivery model, the IT workforce will be aligned according to the new organizational model. This alignment will follow a logical and predictable path that minimizes the impact on bureau operations.

---

## 8 Managing Information as an Asset

### 8.1 Supporting Interoperability and Openness (GXXA)

Section 206 of the E-Government Act of 2002 requires each agency, to the extent practical, to: (1) ensure that a publicly accessible federal government website includes all information about that agency required to be published in the Federal Register under the Freedom of Information Act, (2) accept submissions under 5 U.S.C. 553(c) by electronic means, and (3) ensure that electronic rulemaking dockets are made publicly available through a federal government website. Sections 207(f) and 208(c) require OMB to issuance guidance for agency websites.

DOI has a publicly accessible federal website that includes all information about the Department required to be public in the Federal Register/FOIA. Additionally, each bureau within DOI maintains a FOIA website and may also have specific FOIA Reading Rooms containing frequently requested DOI-implemented requirements of Section 206 by September 2005, which was the deadline established by OMB in its 2003 annual report to Congress. Examples of actions taken, including all rulemaking documents, are automatically included in the daily feed sent to [www.regulations.gov](http://www.regulations.gov) by the Federal Register. DOI posts these documents soon after they are received in a public domain directory of public federal government websites (207(f)(3)) that they developed and established. Interior is currently in the process of updating its list of public federal government websites and the domain names under its control as it actively seeks to reduce these numbers.

DOI complies with OMB guidance for privacy notices on agency websites. The Department of the Interior (DOI) Web Standards Handbook (386 Departmental Manual 3) requires that DOI and bureaus comply with laws and directives regarding the protection of privacy data on DOI and bureau websites. All official DOI and bureau website pages must link to the DOI Privacy Policy, which is posted on the official DOI website. The Privacy Policy provides information to the public on what information is collected; the purpose of the collection; how that information is handled, used, and shared; how information from the use of social media applications is handled and shared; the DOI linking policy; and website security controls used to protect information. DOI and bureau web pages that collect information directly from individuals must provide a privacy notice that specifically addresses the requirements of the privacy provisions of Section 208 (c).

#### Public Access to Electronic Information

Section 207(e) of act required NARA to issue policies requiring agencies to adopt policies and procedures to ensure that records management requirements are applied effectively. The Department is developing an enterprise-wide forms system that will incorporate records management and other information management policies and procedures into standard forms with associated workflow processes and standardized file formats that will leverage existing technology and reduce costs.

Section 207(g) of the act required agencies to provide information required to populate the repository that contains information about research and development funded by the federal government. The Department is developing an enterprise electronic and records management system. This system will populate metadata fields for electronic records. In addition, it will assign and categorize the appropriate records schedule and disposition.

---

Since 2005, DOI has continued actions to integrate electronic information collection to reduce burdens, create interoperability in databases among agencies, and improve the utility and accessibility of government information. Specific actions include:

- Established performance measures of Open Government progress including number of Interior datasets available on data.gov, reduction of Freedom of Information Act (FOIA) backlog, and level of participation in Open Government-focused initiatives.
- Enhancing public participation in government by electronic means by using [www.Regulations.gov](http://www.Regulations.gov) as the central access and dissemination point for all regulations and related documents.
- Continuing to perform as an established Government-wide Managing Partner for Geospatial One Stop, Geospatial Line of Business (LoB), Recreation One Stop (through the third quarter of 2010), as well as a Shared Service Provider for both Human Resource and Financial Management LoBs.
- Performing as a Supporting Partner for sixteen E-Government initiatives and six Lines of Business (LoBs) to develop common solutions where government-wide efficiency and reduced costs can be achieved.

## **8.2 Controlling Accessibility to Personal Information (GXXB)**

---

The DOI Chief Information Officer is the Senior Agency Official for Privacy and, as such, has the primary authority and responsibility for overseeing an agency-wide privacy program and implementing policies and procedures to ensure agency compliance with all applicable privacy laws, regulations, policies, and standards. DOI is committed to building a privacy program focused on protecting individual privacy in alignment with the DOI mission to build a 21<sup>st</sup> century Interior.

DOI's mission diversity and geographic dispersion make risk mitigation a challenging and complex undertaking. With Secretarial Order 3309, DOI initiated a reorganization of the technical, financial, and cultural structure of the organizational subcomponents. This reorganization has enabled DOI to better facilitate collaboration across information management and assurance programs that will result in improved overall compliance for the safeguarding of individual privacy and sensitive Personally Identifiable Information (PII). In order to ensure compliance with the Privacy Act of 1974, E-Government Act of 2002, and other Federal laws and to improve utilization of resources to assure appropriate safeguards to protect personal information, the new centralized Departmental Privacy Program within the Office of the Chief Information Officer will enable the consolidation of compliance activities across the enterprise, reduce duplicative or inconsistent policies and procedures, and ensure uniform implementation of controls and best practices to protect sensitive PII throughout the information lifecycle in accordance with applicable privacy laws, regulations, policies, and standards.

Privacy governance strategy is focused on ensuring appropriate safeguards to protect PII and the confidentiality, integrity, and availability of information assets. DOI has implemented a combination of technical, administrative, and physical controls to safeguard personal information from inappropriate or unauthorized access, use, or disclosure in alignment with Federal mandates and National Institute of Standards and Technology (NIST) guidance and standards for the protection of sensitive PII and SBU information. DOI's Information Security Program ensures compliance with the Federal Information Security Management Act (FISMA) and uses operational controls and privacy enhancing technologies such as data loss prevention software, data anonymization, encryption, firewalls, authorized use system access controls (such as Multi-Factor authentication with Smart Cards), and system audit logs. DOI has effectively reduced the risk of loss or

---

compromise of sensitive PII in agency communications by implementing a Data Loss Prevention (DLP) solution that monitors network communications and prevents sensitive PII from leaving the network.

In addition to these technical controls, administrative controls utilized at DOI include policies and procedures at the component or system level to control access to personal information, such as DOI Privacy Act regulations, Departmental Manual Privacy Chapters, Rules of Behavior, and privacy training and awareness. DOI Privacy Act regulations at 43 CFR Part 2 implement the provisions of the Privacy Act and outline roles, responsibilities, and requirements for the collection, maintenance, and disclosure of records subject to the Privacy Act. Additionally, the regulations also require minimum physical safeguards to ensure the security and confidentiality of records subject to the Privacy Act, including limiting physical access to protected records and restricted access to file cabinets and DOI facilities where records are stored.

To further mitigate privacy risks, DOI promulgated the DOI Privacy Loss Mitigation Strategy (PLMS), which outlines procedures for the protection of PII, the reporting of lost or compromised PII, and remedial steps to mitigate any impact to affected individuals following a privacy incident. DOI promulgated the DOI Privacy Policy for the Information Sharing Environment (ISE), which outlines roles, responsibilities, and requirements for implementing individual privacy, civil rights, and civil liberties protections in the information sharing environment in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004, Executive Order 13388, and the ISE Privacy Guidelines.

DOI conducts Privacy Impact Assessments (PIA) on all information systems, third-party websites, and social media applications in accordance with the E-Government Act and OMB policy to demonstrate that the agency has evaluated privacy risks and incorporated protections commensurate with those risks to safeguard the privacy of personal information. The DOI PIA Guide provides guidance and outlines requirements for completing PIAs to ensure that PII is only collected as authorized, that system of records notice (SORN) requirements are met, and that appropriate security controls are implemented to protect and manage access to PII within DOI information systems. As part of the DOI PIA compliance review cycle, PIAs are updated whenever changes occur to the information system or process or every three years. This ensures privacy implications are addressed when planning, developing, implementing, and operating information systems that maintain information on individuals.

The DOI Privacy Office also conducts data calls and compliance reviews on PIA and SORN inventories, as well as DOI websites, portals, and forms, to assess compliance with privacy laws, policies, and standards; increase accountability; and promote a culture of privacy compliance within DOI. In order to meet the mission of the DOI Privacy Program, to provide privacy policy and compliance leadership in promoting and protecting privacy and transparency, the DOI Privacy Program will meet the following objectives:

- Issue policies and provide guidance to DOI bureaus and offices on requirements for privacy protection through guidelines, templates, and forms to comply with Federal privacy laws, regulations, and policies, while promoting the Fair Information Practice Principles (FIPPs).
- Conduct privacy compliance reviews annually on existing programs, systems, projects, information sharing arrangements, and other initiatives to reduce the impact on individual privacy and ensure compliance with Departmental privacy policy and the FIPPs.

- 
- Collaborate with other Federal agencies and partners to advance the FIPPs and foster a culture of privacy and transparency through policy and partnerships to fulfill the DOI's mission as it relies on interagency cooperation.
  - Ensure privacy incidents are reported, investigated as appropriate, and mitigated in accordance with Federal and DOI policies and plans.
  - Build a privacy outreach, education, and awareness campaign to promote privacy, develop privacy training courses, and disseminate materials to employees and contractors as appropriate.

To achieve these goals and ensure privacy is properly protected, DOI is revising DOI Privacy Act regulations and Departmental Manual Privacy chapters (383 DM 1-13) to reflect new Federal requirements, updated DOI privacy policies, and new NIST standards and privacy controls for the handling, sharing, and protection of sensitive PII. In order to increase privacy awareness and ensure compliance with Federal privacy laws and updated DOI privacy policies, the DOI Privacy Training Program has developed a robust privacy curriculum that includes mandatory privacy training that is delivered as part of the Federal Information System Security Awareness (FISSA) training that must be completed by all employees and contractors annually. In addition, a series of ten role-based privacy training courses for specialized groups with PII responsibilities will be deployed over the next three years. Initial targeted, role-based training courses include Privacy for IT Personnel, Privacy for HR/EEO Professionals, Privacy for the Information Sharing Environment, Privacy for System Managers, and Privacy for Information Management Personnel.

---

## 9 Commodity IT and Shared Services

### 9.1 Maturing the IT Portfolio (HXXA)

---

Interior is currently performing a hosting study to evaluate the hosting operations that are currently being managed and performed by subcomponent organizations. The study will evaluate the current hosting capabilities and define a future state hosting shared service business model. In parallel to the study, an application rationalization initiative is being performed to evaluate the current DOI application portfolio, evaluate ways to improve support for each line of business, and assist in the strategic direction of hosting services to include simplifying infrastructure and creating the most efficient model related to resourcing that service area as well as other IT service lines. The initiatives to support hosting services, such as data center consolidation, moving applications/services to the cloud, and standardizing on infrastructure, are all efforts supporting Interior's strategic direction in support of optimizing IT infrastructure, rationalizing applications, and adopting a service oriented approach in providing shared services.

It is expected that by FY 2014, hosting services will be managed by OCIO to include the reprogramming of workforce from bureau/office to DOI OCIO/ITSSO as well as those infrastructure assets that are considered within the scope of Hosting Services. Other activities associated with the stand-up of hosting shared services include:

- Aggressive closure of 40% of non-core data centers based on future guidance that will be provided by OMB Federal Data Center Consolidation Initiative (FDCCI).
- Identification of 30-50% of DOI applications/services that could be migrated to a public cloud service within the next five years.

A Foundational Cloud Hosting Services Contract is expected to be awarded in May 2013 with the first task orders being submitted in FY2013 Quarter 4. Services provided by this contract vehicle include storage, secure file transfers, virtual machines, database hosting, development and testing environments, and web hosting.

The Department of the Interior (DOI) recently completed an acquisition of and migration to a cloud-based "Software as a Service" (SaaS) email and collaboration service from a commercial provider of Cloud Computing services for over 70,000 employees. Interior's goal was to transition its legacy email and collaboration services from disparate, on-premise systems to a highly integrated, innovative, creative, cost-effective, and evolving cloud-based environment. The new service provides an integrated suite of tools and capabilities that allows Interior to transform the way business is conducted while also maintaining the ability to manage and monitor service performance, quality, and delivery through clearly defined roles and business rules rather than through physical control of assets and direct software licensing.

The cloud-based solution increases employee productivity and collaboration and improves its service to the American people. The primary objective of the cloud-based email and collaboration services acquisition was to reduce DOI's service delivery costs as well as to equip and empower DOI employees with secure, modern, reliable communication. The resulting capabilities act as a catalyst to accelerate and improve the delivery of mission goals and services in the future. Primary outcomes of this initiative include:

- Modernizing DOI's e-mail system.

- 
- Provisioning services in a government community or private cloud solution that include email, calendaring, cloud-based email archiving/journaling, instant messaging, desktop video conferencing, web-based collaboration systems, and support for connecting mobile devices.
  - Reducing the government's in-house system maintenance burden and associated spending.
  - Ensuring appropriate security and privacy safeguards.

Interior is currently in the planning and design phase of an Enterprise Directory Services (EDS) project to re-architect the DOI directory service environment into a single-forest, three-domain architecture that is designed around technology boundaries rather than organizational boundaries. This solution has the benefit of realizing operational efficiencies, increased security, and economy of scale.

The DOI Directory Services environment has been actively operating for more than seven years and has settled into a functional steady-state operations model, with the respective bureau child domains operating at varying levels of efficiency and standardization. More specifically, the current architecture was implemented based entirely on organizational boundaries and consequently segmented into bureau and office domains with unnecessary complexity, duplicative administration, and other unwarranted costs. The Single Forest option for the transformation of the Enterprise Directory Services proposes implementing architecture with a single forest and three separate domains (SF3D) that address operational and security deficiencies. The first is a forest root domain which will have limited scope in services and only contains those services which are central to the enterprise functions and appropriate for placement within the root domain. The second domain will contain most user and workstation related objects while the third will host enterprise-level resources which are utilized and accessed by a variety of customers.

Moreover, this alternative supports the implementation of separate sites for the bureaus as needs and Global Policy Objects that restrict the rights of site administrators and apply the GPO at each site. The single forest 3 domain model inherently increases the Department's ability to ensure compliance, provides the ability to effectively audit directory objects and actions, and increases security by significantly reducing the number of Domain Administrators with full access to domain functions.

The DOI Unified Telecommunications Services Program will provide modern, cost-effective, consolidated telecommunications services (WAN, LAN, Voice, Video, Radio, and Cellular) to the Department's bureaus and offices, consistently exceeding customer satisfaction and operational expectations. DOI's Unified Telecommunications Services Program provides consolidated enterprise-wide WAN, LAN, Voice, Video, Radio, and Cellular capabilities in response to DOI, bureau/office, and local-level telecommunication needs. UTSP provides common telecommunication tools to assist DOI operational components achieve their missions as demonstrated in Figure 3: UTSP Services below.



Figure 7: UTSP Services

## 9.2 Reinvesting Savings from Commodity IT Consolidation (HXXB)

Interior plans on capturing savings generated by the consolidation of IT infrastructure and other streamlining efforts and reinvesting those savings into subsequent phases of IT transformation, such as migration of applications/services to the cloud. Related specifically to hosting services:

Interior is working closely with its subcomponent organization to meet OMB requirements and mandates. Interior committed to closing 95 data centers by 2015 and has currently closed 48 data centers and is ahead of schedule. Interior is also working closely with OMB to meet FDCCI requirements related to the identification of Core and Non-Core data centers and in May will begin the planning associated with the closure of 40% of Interiors Non-Core facilities (approximately 120 data centers).

Interior is also working to establish enterprise contracts for commodity IT, specifically focusing on contracts where large volumes of licenses are required in all shared service areas such as virtualization, system software, and support services. This and standardizing on technology such as virtualization, hardware platforms, and software are just two of the large pushes for DOI. Standardization supports more efficient workforce models, assists with training requirements, and support services.

Interior is aggressively seeking opportunities to leverage cloud services. Services that have already been established include the implementation of an Interior-wide, cloud-based email and collaboration system to include instant messaging, desktop video conferencing, and messaging archiving. DOI is currently in the acquisition phase of acquiring cloud-based hosting services.

Specifically related to Interior's cloud-based email and collaboration system, Interior expects to realize costs savings and/or avoidance at the Bureau/Office sub-organization component level through decommissioning of legacy email systems, reducing the need to maintain separate hardware, software, and administrative support components for the legacy email systems. These cost savings can be reinvested into the bureau/office mission.

Similarly to the cloud-based email and collaboration system, Interior's Enterprise Directory Services Consolidation plan will also enable reductions in hardware, software, and administrative support costs, as well as implement standardization across the enterprise, resulting in reinvestment opportunities at the bureau/office level.

Other ways DOI plans to reinvest savings are listed below.

- Accelerate and expand strategic sourcing agreements for expanded network services: Video, Voice, Radio, and Cellular.
- Define and implement a Unified Telecommunication Services Program central and regional support structure that utilizes existing DOI telecommunications specialists and service provider resources.
- Implement a robust training program for UTSP personnel to include core business requirements such as contracting, budgeting, finance, administrative, and human resource management.
- Converge Wireless, Wireline, Cellular, Video, Voice, Radio, and IT Infrastructures.
- Expand Managed Services for local area network infrastructure operations and maintenance.
- Establish Enterprise Voice, Video, Radio, and Cellular appropriations line items.
- Establish Enterprise-wide oversight authority over telecommunication acquisitions including Voice, Video, Cellular, and Radio.

### 9.3 Maximizing Use of Inter- and Intra-Agency Shared Services (HXXC)

Where appropriate, DOI reaches out to other agencies to leverage excellent work or lessons learned in regards to shared services. Interior is actively engaged in the Federal Data Center Consolidation Initiative (FDCCI) and, as such, works closely with other federal agencies regarding shared service offerings specific to data center offerings and seeking opportunities to leverage existing services where appropriate (contract vehicles, data center facilities, etc.). Where services are not available, Interior will create contract vehicles or opportunities for other agencies to leverage or partner with Interior.

Interior is one of many Federal agencies that have transitioned to the Google Apps for Government cloud email and collaboration service. Interior has established a shared services support model for managing the service, including development of a centralized support model, standard Service Level Agreements, and management of the service provider integration and support contract. Additionally, Interior initiated a bi-monthly meeting with Google executives and CIO representation of all other Federal agencies using Google Apps for Government. Technical sub-teams have evolved out of the executive-level meetings to address common issues and concerns across the Federal sector. The sub-teams are working collaboratively to identify and escalate opportunities for increasing security, functionality, and collaboration with the Google service and between other Federal agencies.

Interior's Enterprise Directory Services project to re-architect the DOI directory service environment into a single-forest, three-domain architecture has the benefit of realizing operational efficiencies, increased security, and economy of scale. Tasks currently performed by the bureaus/offices will be subsumed by OCIO Directory Services Administrative staff, in a shared services model, during and after the EDS project. This will eliminate the need for bureaus to do the following, included but not limited to:

- Domain Controller monitoring and maintenance.
- DNS management for DOI.NET (and child) namespace.
- Support Internal Directory Service integrated DNS Servers and name resolution.
- Support existing and new sites/services.
- Create and enforce standard DOI policy objects.
- Manage forest and domain trusts.
- Top level organizational unit (OU) creation, delegation, and maintenance.

- 
- Ensure proper and timely replication of data between Domain Controllers.
  - Perform forest audit type functions.
  - Integration and engineering functions related to new and existing enterprise applications.
  - Tier 3 troubleshooting assistance.

For FY14, the Geospatial Platform has been formally introduced as one of the OMB eGovernment Shared IT Services. The Department serves as the Federal leader in the development and refinement of the Government-wide Geospatial Platform ([www.geoplatform.gov](http://www.geoplatform.gov)), an interagency initiative led by the Assistant Secretary for Water and Science and the Department's Geospatial Information Officer. The Department has also lead the collaborative development of a landscape Decision Tool to support policy development and decision making through the use of shared data and analysis utilizing geospatial resources from Federal, State, and local governments as well as Non-Government Entities.

#### **9.4 Critical Application COOP (HXXD)**

---

Currently DOI and its subcomponent organizations provide the proper continuity of operations (COOP) and disaster recovery (DR) capabilities based on the specific requirements of a particular application. DOI is actively pursuing additional means in which COOP and DR requirements can be met more efficiently by utilizing shared resources across all DOI bureaus/offices as well as leveraging other technologies (cloud-based offerings). From a shared services perspective one of the requirements moving forward with any strategy is the consideration for COOP and DR to meet the mission needs of all DOI as well as subcomponent organizations.

DOI's cloud based email and collaboration service takes advantage of the COOP and DR capabilities provided by our Cloud services vendor. The Statement of Objectives for our cloud email services requirement specifically includes language to ensure requirements are included to prevent the loss of DOI data, service degradation, and/or service disruption to DOI users in the event of planned or unplanned outage. To address this, the cloud based vendor is providing:

- multiple copies of user data are made available in real-time to the various Google services through live (or synchronous) replication
- every action taken in Gmail is simultaneously replicated across multiple servers in at least two data centers
- if a server fails or an entire data center suffers an interruption, there is nearly instantaneous transfer of data over to another
- RPO design target is zero
- RTO design target is instant failover

#### **9.5 Web Services, Mobile Optimization and Digital Services (HXXE)**

---

Interior is committed to the continuous improvement and innovative application of modern automation, communication and collaboration technologies our employees, partners, collaborators, other agencies, and the American people expect of twenty first century Government. Web services and, increasingly, mobile

---

technologies and applications have the power to transform the way we conduct and communicate the diverse missions of the agency's bureaus and offices.

OMB's Digital Government Strategy requires all agencies to undertake actions to optimize customer facing services for mobile devices and services and make available "high-value" data and content over the Web using common APIs. Interior's Enterprise Mobility Strategy provides a framework to ensure that DOI develops mobile solutions that improve customer service and provide more universal access to information utilizing an increasingly broad array of devices. The agency's Web Strategy is similarly focused on optimizing Interior's use of Web technologies to improve employee productivity in support of the mission, foster greater transparency, improve public and partner collaborative capabilities, and encourage consumption of Interior's broad, publicly available information sets.

Interior's Enterprise Mobility Strategy provides the high level context to address these demands and identifies initiatives to support DOI strategic goals through and effective adoption of mobility goals and objectives. Details for the initiatives are addressed in companion implementation guidance documents tailored for specific purposes. These implementation planning documents will reference the goals, objectives and initiatives identified in this strategy and also map to the Digital Government Strategy. The Enterprise Mobility Strategy prioritizes DOI's customer base, recognizing the complimentary relationship between the OMB strategy and DOI customer demand.

The Department's Web Strategy, which is outlined in its Departmental Web Manager's Handbook, provides guidelines for bureaus and offices to manage Web sites and content. The Department continues to develop and update policy and procedures to appropriately govern its Web sites in order to ensure compliance with open data, content, and web API policies.

**Web, Digital Services and Mobile Optimization Core Principles:**

- We will establish standards and development practices that support platform independence to enable flexibility and reuse of data and system functionality
- We will promote the adoption of technologies that benefit our employees in support of the mission, while advancing our communication and collaboration capabilities with our partners and the American people
- We will maintain a strong focus on risk based security measures that coincide with the sensitivity of DOI information
- We will develop mobile capabilities that enable sound records management practices and legal discovery requirements
- We will seek to leverage existing capabilities where practical and cost-effective
- We will adopt a continuous, incremental improvement process into our strategy to monitor platform trends, innovative uses and best practices in service delivery and data protection
- We will approach a mobile strategy as an enterprise initiative to be coordinated across the entire Department and with appropriate prospective partners
- We will make content and high-value data available to our partners and the American people using common APIs, mobile-friendly applications and innovative Web services

---

Interior's approach to modernizing its existing systems to leverage Web services and optimize for mobile usage is tightly coupled with its IT Transformation plan. The agency's Hosting initiative, one of several major cost saving and optimization efforts begun in 2012, will afford Interior the opportunity to leverage cloud-based infrastructure and complete platforms for its Web services. Through application rationalization, also a part of this initiative, Interior will achieve a reduction in the number of duplicative services and applications allowing us to target key remaining applications for modernization and optimization. To improve digital services to our partners and the public, DOI has partnered with its bureau and office program managers to identify high-value data sets and work together to make these available through Web APIs.

This work has already begun. In late 2012, Interior introduced for its employees a Web based application "store" that provides access to the agency's legacy time and attendance system, its online learning system, and its Intranet through a single portal that is accessible anywhere and at any time. In support of the Digital Government Strategy, DOI has developed and made available, or will shortly make available, wildlife, hydrography, earthquake, wetlands, and mapping and land use data using Web APIs. As the list of services available to the public continues to grow, Interior has established a Developer "Hub" for our data consumers. Links to more than 20 of these resources can be found at <http://www.doi.gov/developer>. Demonstrating our commitment to mobile technologies to showcase our mission and services, several applications are now available for iOS and/or Android devices from USGS, FWS, and NPS. These applications are regularly updated reflecting the feedback and experiences of consumers. Interior continues to explore new and innovative ways to bring data and interpretive services to the mobile devices of the American people.

In 2012, Interior instituted a bureau and office spend plan review process that allows Office of the Chief Information Officer staff to confirm that spending on new or existing systems and services is aligned with broader IT Transformation initiatives and Secretarial Order 3309, in addition to other requirements and mandates. This process has also allowed OCIO to successfully assess new systems for compliance with open data, content, and Web API policy and ensure alignment with both OMB and DOI Digital Services strategy.

DOI is currently in the process of developing a Mobility Strategy to help focus and align a wide array of efforts associated with mobility. The following elements are being considered for the final version of that strategy.

### **Mobile Device Strategy – Goals and Objectives**

#### **Goal:**

- Enhance DOI's ability for anywhere, anytime anyplace computing through the expanded use of platform independent web-based solutions and mobile technologies that balance the value of flexible access and risk.

#### **Objectives:**

#### **Adopt mobile first design strategy in all new development**

DOI applications and information services will be designed for the Web and include consideration for mobile device access. Core tenets include platform and browser independence, separation of data from process and user interface (note this is also in alignment with the Digital Government Strategy and Shared Services Strategy) and publication of agency data to the cloud where it can be readily repurposed.

---

### **Enhance DOI App store to serve as a central clearinghouse for all DOI web-based and mobile applications**

Establish policy that requires all DOI developed web and mobile solutions to be registered in standard format with the DOI App store. Create public view and position on DOI.Gov.

### **Expand web based and mobile offerings- identify key mobile functions and work to bring them to production**

Identify likely areas for delivering broad based value to DOI's employees and customers.

### **Clarify actions and applications available on government furnished vs. BYOD**

Recognize that not all functions are appropriate for use on non-government furnished equipment. Establish a bright line that separates information and functions that may be performed on BYOD vs. those that require GFE.

### **Establish ongoing risk assessment and mobile environment awareness capabilities to ensure that new developments in web-based and mobile technology are well understood**

New mobile products will be rapidly introduced into our environment. We must monitor major platforms and the mobile environment to ensure we are not accepting unknown risks. We must also continue to collaborate with other agencies and the private sector to identify cost effective ways to improve mobile capabilities.

### **Establish a common platform and infrastructure to promote manageability and risk understanding of mobile access and to promote efficiency and interoperability**

A common platform for all DOI web applications and mobile access will promote ubiquitous access and facilitate seamless integration of mobile and traditional computing. A common platform will also foster the establishment of a DOI mobile community of practice where web and mobile developers can provide peer support to DOI application development.

## **Wireless Services Strategy**

Following the award of its Cloud-based Email and Collaboration Services contract in 2012, Interior has begun to see a significant shift in wireless device usage. With that change in usage comes change in device and, potentially, change in service plan. Historically Interior's wireless contracts have been managed at or below the bureau and office level, making it extremely difficult to maintain an accurate enterprise inventory of devices and sacrificing the potential economies of scale an organization the size of DOI might recognize. The extremely distributed and diverse nature of the Department of the Interior's mission, combined with factors including geographic isolation, a heavy emphasis on field work, and varied, often disparate, funding models has previously thwarted efforts to consolidate wireless contracts. However, our market research indicates that thanks to competition in the market, carrier reach, pooling, and billing models are today more flexible than ever before.

In late 2012, OCIO organized a team consisting of acquisitions, technical experts, and wireless contract managers from representative bureaus to formulate a strategy for the creation of one or more enterprise wireless contracts, with the goal of migrating or consolidating myriad bureau and office contracts into these. Though Interior has been heavily involved in GSA's Federal Strategic Sourcing Initiative for wireless, it is exploring

---

options and formulating an acquisition strategy with an intent to deliver consolidated enterprise wireless and device contract(s) to the Department at large by calendar year end, 2013.

---

## 10 Privacy

### 10.1 DOI's Privacy Approach (IXXA)

The DOI Chief Information Officer is the Senior Agency Official for Privacy and as such, has the primary authority and responsibility for overseeing an agency-wide privacy program, and implementing policies and procedures to ensure agency compliance with all applicable privacy laws, regulations, policies and standards. DOI is committed to building a privacy program focused on protecting individual privacy in alignment with the DOI mission to build a 21st century Department of the Interior.

DOI's mission diversity and geographic dispersion makes risk mitigation a challenging and complex undertaking. With Secretarial Order 3309, DOI initiated a reorganization of the technical, financial and cultural structure of the organizational subcomponents. This reorganization has enabled DOI to better facilitate collaboration across information management and assurance programs that will result in improved overall compliance for the safeguarding of individual privacy and sensitive PII. In order to ensure compliance with the Privacy Act of 1974, E-Government Act of 2002, and other Federal laws, and improve utilization of resources to assure appropriate safeguards to protect personal information, the new centralized Departmental Privacy Program within the Office of the Chief Information Officer will enable the consolidation of compliance activities across the enterprise, reduce duplicative or inconsistent policies and procedures, and ensure uniform implementation of controls and best practices to protect sensitive PII throughout the information life cycle in accordance with applicable privacy laws, regulations, policies and standards.

Privacy governance strategy is focused on ensuring appropriate safeguards to protect PII and the confidentiality, integrity and availability of information assets. DOI has implemented a combination of technical, administrative and physical controls to safeguard personal information from inappropriate or unauthorized access, use, or disclosure in alignment with Federal mandates and National Institute of Standards and Technology (NIST) guidance and standards for the protection of sensitive PII and SBU information. DOI's information security program ensures compliance with the Federal Information Security Management Act (FISMA) and uses operational controls and privacy enhancing technologies, such as data loss prevention software, data anonymization, encryption, firewalls, authorized use system access controls (such as Multi-Factor authentication with Smart Cards), and system audit logs. DOI has effectively reduced the risk of loss or compromise of sensitive PII in agency communications by implementing a Data Loss Prevention (DLP) solution, that monitors network communications and prevents sensitive PII from leaving the network.

In addition to these technical controls, administrative controls utilized at DOI include policies and procedures at the component or system level to control access to personal information, such as DOI Privacy Act regulations, Departmental Manual Privacy Chapters, Rules of Behavior, and privacy training and awareness. DOI Privacy Act regulations at 43 CFR Part 2, implement the provisions of the Privacy Act and outline roles, responsibilities and requirements for the collection, maintenance, and disclosure of records subject to the Privacy Act. Additionally, the regulations also require minimum physical safeguards to ensure the security and confidentiality of records subject to the Privacy Act, including limiting physical access to protected records, restricted access to file cabinets and DOI facilities where records are stored.

To further mitigate privacy risks, DOI promulgated the DOI Privacy Loss Mitigation Strategy (PLMS) which outlines procedures for the protection of PII, reporting of loss or compromised PII, as well as remedial steps to

---

mitigate any impact to affected individuals following a privacy incident. DOI promulgated the DOI Privacy Policy for the Information Sharing Environment (ISE), which outlines roles, responsibilities, and requirements for implementing individual privacy, civil rights and civil liberties protections in the information sharing environment in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004, Executive Order 13388, and the ISE Privacy Guidelines.

DOI conducts Privacy Impact Assessments (PIA) on all information systems, third-party websites and social media applications in accordance with the E-Government Act and OMB policy, to demonstrate that the agency has evaluated privacy risks and incorporated protections commensurate with those risks to safeguard the privacy of personal information. The DOI PIA Guide provides guidance and outlines requirements for completing PIAs to ensure that PII is only collected as authorized, that system of records notice (SORN) requirements are met, and that appropriate security controls are implemented to protect and manage access to PII within DOI information systems. As part of the DOI PIA compliance review cycle, PIAs are updated whenever changes occur to the information system or process, or every three years. This ensures privacy implications are addressed when planning, developing, implementing, and operating information systems that maintain information on individuals.

The DOI Privacy Office also conducts data calls and compliance reviews on PIA and SORN inventories, as well as DOI websites, portals and forms, to assess compliance with privacy laws, policies and standards, to increase accountability, while promoting a culture of privacy compliance within DOI. In order to meet the mission of the DOI Privacy Program to provide privacy policy and compliance leadership in promoting and protecting privacy and transparency, the DOI Privacy Program will meet the following objectives:

- Issue policies and provide guidance to DOI bureaus and offices on requirements for privacy protection through guidelines, templates, and forms to comply with Federal privacy laws, regulations, and policies, while promoting the Fair Information Practice Principles (FIPPs).
- Conduct privacy compliance reviews annually on existing programs, systems, projects, information sharing arrangements, and other initiatives to reduce the impact on individual privacy and ensure compliance with Departmental privacy policy and the FIPPs.
- Collaborate with other Federal agencies and partners to advance the FIPPs and foster a culture of privacy and transparency through policy and partnerships to fulfill the DOI's mission as it relies on interagency cooperation.
- Ensure privacy incidents are reported, investigated as appropriate, and mitigated in accordance with Federal and DOI policies and plans.
- Build a privacy outreach, education and awareness campaign to promote privacy, develop privacy training courses, and disseminate materials to employees and contractors as appropriate.

To achieve these goals and ensure privacy is properly protected, DOI is revising DOI Privacy Act regulations and Departmental Manual Privacy chapters (383 DM 1-13) to reflect new Federal requirements, updated DOI privacy policies, as well as new NIST standards and privacy controls for the handling, sharing and protection of sensitive PII. In order to increase privacy awareness and ensure compliance with Federal privacy laws and updated DOI privacy policies, the DOI Privacy Training Program has developed a robust privacy curriculum that includes mandatory privacy training that is delivered as part of the Federal Information System Security Awareness (FISSA) training that must be completed by all employees and contractors annually. In addition, a series of ten

---

role-based privacy training courses for specialized groups with PII responsibilities will be deployed over the next three years. Initial targeted role-based training courses include Privacy for IT Personnel, Privacy for HR/EEO Professionals, Privacy for the Information Sharing Environment, Privacy for System Managers and Privacy for Information Management Personnel.

---

## **11 Accessibility**

### **11.1 Creating a Diverse Work Environment (JXXA)**

---

DOI is committed to building and maintaining a diverse environment, integrating accessibility considerations into IT processes, and developing workforce skills to support Section 508 requirements. In alignment with the DOI mission to build a 21<sup>st</sup> century Interior, the DOI CIO's goal is to provide cost-effective, reliable, and accessible IT products and services to promote a diverse workforce and encourage communication and collaboration between employees, stakeholders, and the public.

As more individuals with disabilities join the Federal workforce, it is imperative that DOI remain effective and responsive for a well-prepared and skilled workforce while providing equal access to Federal government information technology and data. An essential component of such access is to ensure that all electronic and information technology (EIT) developed, procured, maintained, and used within the organization are accessible to individuals with disabilities as mandated by Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d), as amended, the Access Board standards, and other Federal laws and regulations.

DOI employs over 70,000 employees that perform a variety of duties requiring highly-skilled and unique abilities to support the Department's bureaus and offices. Employees are challenged by a decentralized organization and the demands of technology and knowledge management. To address these challenges, the Department is focused on improving key areas that will allow individuals of all abilities to work, interact, and develop into leaders to promote recruitment, improve retention, promote employee development, and maintain an exceptional workforce.

### **11.2 Integrating Accessibility into IT Processes (JXXB)**

---

The Department's vision for a highly-skilled, diverse workforce includes a strategy that uses multiple background factors as tools for competition and workforce development. Differences in background, education, and experience contribute to the varied perspectives in the workplace and create a dynamic environment for higher performance and success in achieving mission goals. The diversity of the workforce requires the DOI CIO to focus on accessibility of EIT that is being developed, procured, maintained, or used. Consistent and close collaboration is vital among employees who define requirements, acquire and manage goods and services, and develop information. It is critical that Section 508 requirements are considered throughout the acquisition and information technology life cycles in order to provide the tools and technology that support a diverse Federal workforce.

### **11.3 Building Workforce Skills to Support Section 508 Compliance (JXXC)**

---

In order to ensure consistent implementation and compliance with Federal laws, DOI initiated a reorganization under Secretarial Order 3309 to enable better collaboration across information management programs. Within this new structure, the DOI Section 508 Program will be consolidated and centrally managed by the Office of the Chief Information Officer. This will allow the Section 508 Program to improve compliance activities across the enterprise and increase efficiencies, resulting in uniform and consistent implementation of Section 508 requirements and best practices. It is in this framework that the DOI CIO will work with functional areas to develop a workforce plan to ensure that the appropriate resources and skill targets are established to deliver the goals and objectives effectively and address the changing technical environment that supports the DOI mission.

---

The Section 508 Program will focus on providing strategic direction, technical support, and training to ensure DOI employees with disabilities have equal access to information technology and data. To accomplish this mission, the Section 508 Program will meet the following objectives:

- Establish enterprise-wide accessibility testing and provide results in a central repository to ensure a standard testing process and procedure and a comprehensive understanding of the Section 508 requirements.
- Review DOI websites and procurement solicitations to ensure accessibility and Section 508 compliance.
- Develop and maintain a training program for web managers, procurement officials, IT managers, and human resource representatives to increase awareness of Section 508 requirements and EIT accessibility.
- Publish Section 508 policies and procedures which will be reviewed annually and updated as necessary to ensure compliance with Federal laws and regulations.
- Establish a centralized location for posting best practices and lessons learned. The DOI Section 508 website and SharePoint Portal will serve as a communication medium for bureaus and offices to share information.